Listing of Claims (including amendments and status):

1   1. (Currently amended) An X.509 certificate stored on computer readable medium, said
2   certificate capable of supporting more than one cryptographic algorithm with an associated
3   public key, comprising:

4   a signature algorithm and signature for all authenticated attributes using a first
5   cryptographic algorithm;

6   a[[n alternative public key]] first certificate extension [[for]] identifying at least one
7   alternative cryptographic algorithm and providing a respective [[its]] associated public key; and

8   a[[n alternative signature]] second certificate extension [[for]] containing a signature for
9   [[the]] each alternative cryptographic algorithm.

1   2. (Currently amended) An X.509 certificate according to Claim 1, wherein the first
2   cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and
3   the first and second certificate extensions are identified as non-critical.

1   3. (Previously presented) An X.509 certificate according to Claim 1, wherein the certificate can
2   be verified by either the signature for the first cryptographic algorithm or the signature for the
3   alternative signature algorithm.

1   4. (Currently amended) A method for enabling an X.509 certificate to support more than one
2   cryptographic algorithm, with associated public key, said method comprising the steps of:

3   providing the X.509 certificate with a signature algorithm and signature for all
4   authenticated attributes using a first cryptographic algorithm;

Serial No. 09/240,265   3   Docket CR9-98-095

5   providing the X.509 certificate with a[[n alternative public key]] first certificate extension

6   [[for]] identifying at least one alternative cryptographic algorithm and providing [[its]] a

7   respective associated public key; and

8   providing the X.509 certificate with a[[n alternative signature]] second certificate

9   extension which contains a signature for [[the]] each alternative cryptographic algorithm.

1   5. (Currently amended) A method for enabling an X.509 certificate to support more than one

2   cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA

3   and the alternative cryptographic algorithm is elliptic curve and the first and second certificate

4   extensions are indicated as non-critical.

1   6. (Previously presented) A method for enabling an X.509 certificate to support more than one

2   cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either

3   the signature for the first cryptographic algorithm or the signature for the alternative signature

4   algorithm.

1   7. (Currently amended) Computer readable code stored on computer readable media for enabling

2   an X.509 certificate to support more than one cryptographic algorithm in association with a

3   public key, said computer readable code comprising:

4   first subprocesses for providing the X.509 certificate with a signature algorithm and

5   signature for all authenticated attributes using a first cryptographic algorithm;

6   second subprocesses for providing the X.509 certificate with a[[n alternative public key]]

7   first certificate extension for identifying at least one alternative cryptographic algorithm and

8   providing its associated public key; and

9   third subprocesses for providing the X.509 certificate with a[[n alternative signature]]

10   second certificate extension which contains a signature for the alternative cryptographic

11   algorithm.

1   8. (Currently amended) Computer readable code for enabling an X.509 certificate to support

2   more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic

3   algorithm is RSA and the alternative cryptographic algorithm is elliptic curve and the first and

4   second certificate extensions are identified as non-critical.

1   9. (Previously presented) Computer readable code for enabling an X.509 certificate to support

2   more than one cryptographic algorithm according to Claim 7, wherein the certificate can be

3   verified by either the signature for the first cryptographic algorithm or the signature for the

4   alternative signature algorithm.

5   10. In a computing environment, a system for enabling an X.509 certificate to support more than

6   one cryptographic algorithm, said system comprising:

7   means for providing the X.509 certificate with a signature algorithm and signature for all

8   authenticated attributes using a first cryptographic algorithm;

9   means for providing the X.509 certificate with a[[n alternative public key]] first

10   certificate extension [[for]] identifying at least one alternative cryptographic algorithm and

11   providing its associated public key: and

12   means for providing the X.509 certificate with a[[n alternative signature]] second

13   certificate extension which contains a signature for the alternative cryptographic algorithm.

1   11.(Currently amended) A system for enabling an X.509 certificate to support more than one

2   cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA

3   and the alternative cryptographic algorithm is elliptic curve and the first and second certificate

Serial No. 09/240,265   5   Docket CR9-98-095

4   extensions are indicated as non-critical.

1   12. (Previously presented) A system for enabling an X.509 certificate to support more than one

2   cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either

3   the signature for the first cryptographic algorithm or the signature for the alternative signature

4   algorithm.

Serial No. 09/240,265   6   Docket CR9-98-095